UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

Jennifer Greenwald and Cynthia Robbins, On behalf of themselves and all others similarly situated,	*	JURY TRIAL DEMANDED
v.	*	
EQUIFAX, INC., a Georgia corporation	*	CLASS ACTION COMPLAINT CIVIL CASE No:

NOW COME the plaintiffs, Jennifer Greenwald, and Cynthia Robbins, individually and on behalf of themselves and all others similarly situated, who hereby bring this class action suit against Equifax, Inc. ("Equifax" or the "Defendant") and allege on personal knowledge, investigation of their counsel, and on information and belief as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages, and other legal and equitable remedies, resulting from the reckless and illegal actions of Equifax, Inc. ("Equifax") related to an unprecedented massive breach of database security (the "Data Breach"). The Data Breach resulted in over 143 million individuals' – nearly half the population of the United States – Personally Identifiable Information ("PII") being stolen from Equifax's databases. For New Hampshire the affected number is approximately 622,000 people .

2. Equifax's failure to adequately protect consumers' most sensitive information has far reaching implications. The stolen PII includes detailed personal data, including names, social security numbers, birth dates, addresses, driver's license numbers, credit card numbers, bank account numbers, and more.

3. According to Equifax's September 7, 2017, press release, Equifax acknowledged it experienced "a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017."

4. Equifax claims it discovered the breach on July 29, 2017, yet it did nothing to notify affected consumers until September 8, 2017, leaving Plaintiffs and half of America vulnerable to identity thieves. As of the date of the filing of this complaint, Equifax still has not bothered to notify Plaintiffs or Class Members of the Data Breach.

5. Meanwhile, Equifax's top executives were busy protecting themselves, rather than focusing on Plaintiffs' vulnerabilities, selling off millions of dollars of their stock before notifying the public. Other stock trading activity suggests other insiders secretly traded Equifax stock, capitalizing on their knowledge there would be a dramatic decline of the stock following the announcement.

6. The Data Breach was a direct result of Equifax's failure to implement adequate security measures to safeguard consumers' PII. Equifax willfully ignored known weaknesses in its data security, including prior hacks into its information

systems. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems, like Equifax. Inasmuch as Equifax is known to possess a massive amount of our nation's PII, Equifax had a duty to implement effective procedures to avoid a breach of this magnitude. Equifax utterly failed in its duty, causing potential harm of gargantuan proportions – potentially impacting consumers for life.

7. Equifax's failure to adequately protect the PII of Plaintiffs and Class Members will allow identity thieves to commit a variety of crimes that harm victims of the Data Breach. For instance, thieves can take out loans, mortgage property, open bank accounts and credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund, obtain a driver's license or identification card in a victim's name, gain employment in a victim's name, obtain medical services in a victim's name, and/or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other criminals who intend to misuse the information for their gain.

8. As a direct result of Equifax's willful failure to prevent the Data Breach, Plaintiffs and Class Members have been exposed to a significant likelihood of fraud, identity theft, and financial harm, as detailed below, and to a substantial, heightened, and imminent risk of such harm in the near and indefinite future.

9. There is a substantial likelihood that Class Members already have or will become victims of identity fraud given the breadth of information about them that is

now in the hands of criminals. Javelin Strategy & Research reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, ***one in three*** consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal." (emphasis added).

10. Plaintiffs and other members of the class never asked Equifax to store their data. Now, as a result of Equifax's failures, Plaintiffs and Class Members are forced to monitor their financial accounts and credit histories more closely and take extra precautions to guard against identity theft.

11. Plaintiffs and Class Members also have incurred, and will continue to incur, additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the Data Breach's impact on their PII for the remainder of their lives. Going forward, Plaintiffs and Class Members anticipate spending considerable time and money in order to detect and respond to the impacts of the Data Breach.

12. In an effort to minimize the harm it caused, Equifax has offered a year of credit protection using its own company, TrustedID. Yet the offer falls far short. The identity thieves have obtained so much PII they are highly unlikely to cease fraudulent activity after twelve months, and as a result Plaintiffs and Class Members will require a lifetime of credit protection. Moreover, inasmuch as Equifax's incompetence is the cause

of the Data Breach, Plaintiffs and Class Members have zero faith that Equifax's "credit protection company" would be an effective and reliable source of protection.

13. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated New Hampshire residents whose PII was accessed during the Data Breach. Plaintiffs seeks to recover damages, including actual and statutory damages, equitable relief, reimbursement of out-of-pocket losses, other compensatory damages, a lifetime of credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

14. The matter in controversy exceeds $5,000,000, the class is comprised of hundreds of thousands of individuals and both plaintiffs have citizenship diverse from the defendant. Accordingly, this Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). This Court also has federal question jurisdiction pursuant to 28 U.S.C. § 1331.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)-(c) and 1441(a), in that Defendant is deemed to reside in any judicial district in which it is subject to personal jurisdiction at the time the action is commenced; Defendant's contacts and business within this District are sufficient to subject it to personal jurisdiction; and a substantial portion of the acts giving rise to this action occurred in this District to residents of this District.

PARTIES

16. Plaintiff, Jennifer Greenwald, is, and at all times mentioned herein, an individual citizen of the State of New Hampshire and resides in Merrimack County, New Hampshire.

17. Plaintiff Cynthia Robbins is, and at all times mentioned herein, an individual citizen of the State of New Hampshire and resides in Dunbarton, New Hampshire.

18. Defendant Equifax, Inc. is incorporated in Georgia with its headquarters and principal place of business located at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309. It is authorized to do business in New Hampshire with a registered agent of The Prentice Hall Corporation Systems, Inc., 10 Ferry Street S313, Concord, NH 03301.

19. Equifax is one of the major credit reporting agencies in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, as described by Equifax, "[t]he company organizes, assimilates and analyzes data on more than 800 million consumers and more than 88 million businesses worldwide, and its database includes employee data contributed from more than 5,000 employers."

FACTUAL ALLEGATIONS

Equifax's Unprecedented Data Breach

20. Starting in mid-May of 2017 and continuing on for at least ***ten weeks***, identity thieves absconded with half of the United States' citizens' critically sensitive PII while Equifax was asleep at the wheel. Equifax claims it learned of this monster breach

on July 29, 2017. Instead of taking steps to notify consumers on a timely basis, Equifax's executives ran off with millions of dollars in profits selling their shares in the days before they made their massive blunder known.

21. Equifax's computer database and systems were accessed by unauthorized users who stole the PII of approximately 143 million individuals, including names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and certain "dispute documents."

22. Equifax discovered the breach on or about July 29, 2017, but failed to disclose the massive breach to the public until September 8, 2017. As of the date of the filing of this complaint, Equifax has still not notified Plaintiffs of the Data Breach.

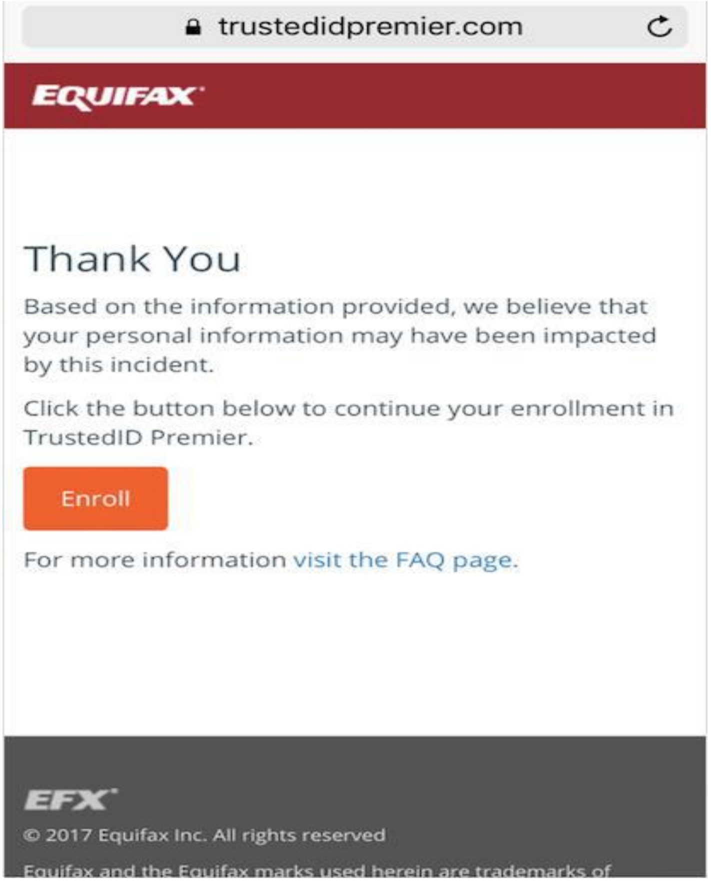
23. Plaintiffs and Class Members have suffered harm as a result of Equifax's negligence and willful ignorance in the form of additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the Data Breach's impact on their PII for the remainder of their lives. Going forward, Plaintiffs and Class Members anticipate spending considerable time and money in order to detect and respond to the impact of the Data Breach.

24. Prior to the Data Breach, Equifax promised to safeguard its consumers' PII: "We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive

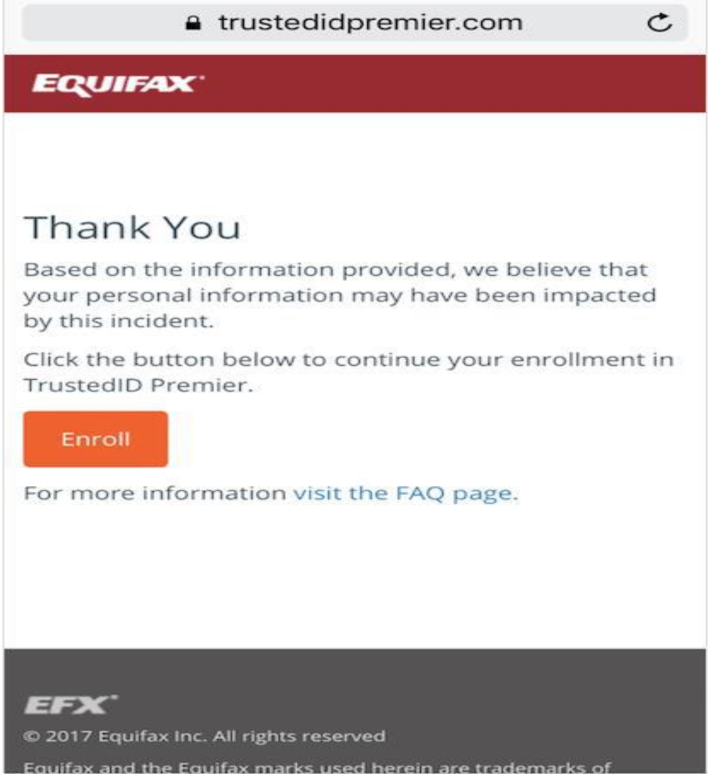
information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is claimed to be a top priority for Equifax." Equifax failed consumers dramatically. 1. http://www.equifax.com/privacy

Plaintiffs' PII Was Fraudulently Used During the Data Breach

25. Jennifer Greenwald: Ms. Greenwald learned about the Equifax data breach like the rest of the world on September 7, 2017. On September 10, 2017, Ms. Greenwald used Equifax's online lookup tool to check and see if her PII was impacted by the Equifax data breach received this message:


trustedidpremier.com
EQUIFAX
Thank You
Based on the information provided, we believe that your personal information may have been impacted by this incident.
Click the button below to continue your enrollment in TrustedID Premier.
Enroll
For more information visit the FAQ page.
EFX
© 2017 Equifax Inc. All rights reserved

26. Cynthia Robbins: Ms. Robbins learned about the Equifax data breach like the rest of the world on September 7, 2017. On September 12, 2017, Ms. Robbins used Equifax's online lookup tool to check and see if her PII was impacted by the Equifax data breach received this message:


trustedidpremier.com
EQUIFAX
Thank You
Based on the information provided, we believe that your personal information may have been impacted by this incident.
Click the button below to continue your enrollment in TrustedID Premier.
Enroll
For more information visit the FAQ page.
EFX
© 2017 Equifax Inc. All rights reserved

27. Upon learning from Equifax that their PII may have been impacted by Equifax's data breach, and while knowing fraudulent activity occurred during the relevant timeframe, Plaintiffs subscribed to credit monitoring programs. Although Equifax offered Plaintiffs free credit protection for a year, Plaintiffs will require a lifetime of credit protection.

28. Moreover, Plaintiffs have no interest in enrolling in a credit protection service with the very company that grossly mishandled their PII in the first place. Plaintiffs and Class Members do not have faith that Equifax's TrustedID credit protection company will be an effective and trustworthy source to guard against identity theft.

29. Plaintiffs are concerned that they will now have to "look over their shoulder" for the rest of their lives, spending time constantly monitoring their credit and banking accounts for fraudulent activity, as a result of the Equifax data breach.

Equifax Was Asleep at the Switch

30. Upon information and belief, Equifax failed to develop, implement, and maintain a comprehensive information security program with administrative, technical, and physical safeguards that were appropriate to its size and complexity, the nature and scope of [its] activities, and the sensitivity of the customer information at issue. This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

31. The Data Breach was a direct result of Equifax's failure to implement adequate security measures to safeguarded consumers' PII and willfully ignored known weaknesses in its data security, including prior hacks into its information systems.

Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax, which are known to possess a massive amount of individuals' valuable personal and financial information.

32. Upon information and belief, Equifax also failed to develop and implement a risk-based response program to address incidents of unauthorized access to customer information in its information systems. This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

33. Equifax failed to timely notify affected consumers promptly after it became aware of unauthorized access to sensitive customer information, and sat on the knowledge for more than a month. As of the date of this filing, Equifax has continued to fail to communicate the Data Breach directly to Plaintiffs and Class Members to date.

34. Equifax also has failed to properly guard against the massive identity thefts which are surely to follow. While Equifax merely offers free credit protection for a year, Plaintiffs and members of the class will require a *lifetime* of credit protection. Equifax is now going to profit generously by the tens of millions of consumers who will begin paying Equifax to continue credit protection at the end of their free year.

Equifax's Failure to Protect PII is Actionable

35. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data

constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, 41.

36. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

37. The FTC also published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

38. The FTC has issued orders against businesses that fail to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

39. By failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

NEW HAMPSHIRE CLASS ACTION ALLEGATIONS

40. Plaintiffs bring all claims as class claims under Federal Rules of Civil Procedure, Rule 23(b)(1), (b)(2), (b)(3), and (c)(4).

41. **New Hampshire Class**: Plaintiffs bring their claims on behalf of New Hampshire consumers, defined as follows:

> II. All natural persons and entities in New Hampshire whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

42. Collectively, all these persons will be referred to as "Class Members." Plaintiffs represent, and are members of the Class. Excluded from the Class are Equifax and any entities in which Equifax has a controlling interest, Equifax's agents and employees, any Judge to whom this action is assigned and any member of such Judge's staff and immediate family, and claims for personal injury, wrongful death and/or emotional distress

43. Plaintiffs reserve the right to amend or modify the class definition after discovery has been conducted.

Certification of the Proposed Classes Is Appropriate

44. Each member of the proposed Class meets the requirements of Fed. R, Civ. P. 23(a), (b)(1), (b)(2), (b)(3) and (c)(4).

45. **Numerosity.** Plaintiffs does not know the exact number of members in the Class but based upon Defendant's September 7, 2017 press release, the Class consists of approximately 143 million individuals of whom several hundred thousand are in New Hampshire. The joinder of all Class Members is impracticable due to the size and

relatively modest value of each individual claim. The disposition of the claims in a class action will provide substantial benefit to the parties and the Court in avoiding a multiplicity of identical suits. The Class can be identified easily through records maintained by Equifax.

46. **Commonality**. There are well-defined, nearly identical, questions of law and fact affecting the Class. The questions of law and fact involving the class claims predominate over questions that may affect individual Class Members. Those common questions of law and fact include, but are not limited to, the following:

a. Whether Equifax failed to adequately safeguard Plaintiffs' and the Class' Personal Information;

b. Whether Equifax failed to protect Plaintiffs' and the Class' Personal Information, as promised;

c. Whether Defendants' computer systems and data security practices used to protect Plaintiffs' and the Class' Personal Information violated federal, state and local laws, or Defendants' duties;

d. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Class' Personal Information properly and/or as promised;

e. Whether Defendants violated the New Hampshire consumer protection statute and data breach notification statutes applicable to Plaintiffs and each of the Class;

f. Whether Defendants failed to notify Plaintiffs and members of the Class about the Equifax Breach on a timely basis after the Equifax Data Breach was discovered, and whether its failure to notify consumers promptly resulted in additional harm.

g. Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Class' Personal Information;

h. Whether Defendants should retain the money paid by Plaintiffs and members of each of the Class to protect their Personal Information beyond the free year offered by Equifax;

i. Whether Plaintiffs and Class Members should receive more than a year of credit protection at no cost.

j. Whether Plaintiffs and the members of the Class are entitled to damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiffs and the members of the Class are entitled to restitution as a result of Defendants' wrongful conduct;

l. What equitable relief is appropriate to redress Defendants' wrongful conduct; and

m. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Class.

47. **Typicality.** All Plaintiffs' claims are typical of the claims of the Statewide Class.

48. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Statewide Class. Plaintiffs have no interests that are adverse to, or in conflict with, the Class Members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, that have sufficient resources to prosecute this action vigorously.

49. **Superiority**. A class action is the superior method for the fair and efficient adjudication of this controversy. The interests of Class Members in individually controlling an individual action are small.

50. Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief with respect to the Class as a whole appropriate.

51. **Injunctive and /or Declaratory Relief**: In addition, Defendants have acted and/or refused to act on grounds that apply generally to the Statewide Class, making injunctive and/or declaratory relief appropriate with respect to the class under Federal Rule of Civil Procedure 23(b)(2). Defendants continue to (1) maintain the PII of Class Members, and (2) fail to adequately protect their PII.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

52. Plaintiffs incorporate all prior paragraphs as if fully set forth here.

53. Equifax owed a duty to Plaintiffs and Class Members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information adequately secured from unauthorized access.

54. Equifax's privacy policy acknowledged Equifax's duty to adequately protect Class Member's PII.

55. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

56. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

57. Equifax owed a duty to disclose the material fact that its data security practices were inadequate in order to properly safeguard Class Member's PII.

58. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach.

59. Equifax had a special relationship with Plaintiffs and Class Members from being entrusted with their PII, which provided an independent duty of care. Plaintiff's and other Class Members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and Class Members' PII from attack not the Class members.

60. Equifax's role to utilize and purportedly safeguard Plaintiffs' and Class Members' PII presents unique circumstances requiring a reallocation of risk.

61. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Member's PII; and (d) failing to provided adequate and timely notice of the breach.

62. But for Equifax's breach of its duties, Class Member's PII would not have been accessed by unauthorized individuals.

63. Plaintiffs and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Plaintiffs and the Class Members.

64. Equifax's negligent conduct provides a means for unauthorized intruders to obtain Plaintiffs' and the Class Member's PII and consumer reports.

65. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures, such as Plaintiffs' purchases of credit protection services and insurance. The unauthorized acquisition of Plaintiffs' and Class Member's PII has also diminished the value of their PII.

66. The damages to Plaintiffs and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

67. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT II

NEGLIGENCE PER SE

68. Plaintiffs incorporates all prior paragraphs as if fully set forth herein.

69. Section 5 of the Federal Trade commission Act ("FTC Act"), 15 U.S.C. § 45 prohibits "unfair...practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by businesses such as Equifax of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form the basis of Equifax's duty.

70. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach in their systems, including specifically the immense damages that would result to consumers.

71. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

72. Members of the Class are within the class of persons Section 5 of the FTC Act was intended to protect as they are individuals engaged in trade and commerce, and bear the risk associated with defendant's failure to properly secure their PII.

73. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and

avoid unfair and deceptive practices, have put consumers' personal data at unreasonable risk, causing the same harm suffered by Class Members.

74. Equifax was further required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

75. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." See 16 C.F.R. § 314.4.

76. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems."

77. Further, when Equifax became aware of " unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation

to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." See *Id*.

78. Equifax violated GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

79. Equifax also violated GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

80. Equifax also violated the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

81. Plaintiffs and Class Members were foreseeable victims of Equifax's violations of the FTC Act and GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and

failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class Members themselves would cause damage to Class Members.

82. Defendants' failure to comply with the applicable laws and regulations, including the FTC Act and GLBA, constitutes negligence per se.

83. But for Equifax's violation of the applicable laws and regulations, Plaintiffs and Class Members' PII could not be accessed by unauthorized individuals.

84. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiffs and Class Members suffered injury, which include but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class Members' PII has also diminished the value of the PII.

85. The damages to Plaintiffs and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations.

86. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT III

VIOLATION OF THE NEW HAMPSHIRE FAIR CREDIT REPORTING ACT

87. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

88. Plaintiffs bring this cause of action on behalf of the New Hampshire class whose PII is maintained by Equifax and/or that was compromised in a data breach announced on September 7, 2017.

89. The Fair Credit Reporting Act requires, in pertinent part, that "consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." NH RSA 359-B:2, I(d). Equifax is a consumer reporting agency under the definition set forth at NH RSA 359-B:3, VI. Plaintiffs and members of the Class are persons and consumers within the meaning of NH RSA 359-B:3, II, III.

90. NH RSA 359-B:4 defines the circumstances under which a consumer reporting agency may furnish consumer reports.

91. NH RSA 359-B:7 establishes compliance procedures requiring consumer reporting agencies to maintain reasonable procedures designed to avoid furnishing consumer reports under any circumstances which are not allowed under 359-B:4.

92. The breach of the personal data of tens of millions of consumers constitutes a violation of the Act's requirement that consumer reporting agencies respect the consumer's right to privacy and that they take reasonable measures to avoid improperly disclosing consumer credit information.

93. Equifax's recklessness in failing to take reasonable measures to protect the confidentiality and privacy of Plaintiffs' consumer reports was, as aforesaid, reckless and therefore willful.

94. NH RSA 359-B:16 gives rise to a private right of action for willful noncompliance and allows for punitive damages.

95. NH RSA 359-B:17 provides a private right of action for negligent noncompliance.

96. Plaintiffs, on their own behalf and on behalf of the Statewide Class, allege that Defendants failed to disclose what specific information was disclosed, what Equifax did or is doing about the unauthorized disclosure of Plaintiffs and Class members' PII, how Plaintiffs and the Class members' could obtain more information about the unauthorized disclosure, and unreasonably delayed in disclosing to Plaintiffs and the Class the breach in security of PII of Plaintiffs and the Class when Defendant knew such information had been acquired by an unauthorized person or persons.

97. As a direct and proximate result of the acts and omissions by Defendants described herein, Plaintiffs and the Class have suffered and/or will suffer significant economic harm including the costs associated with, *inter alia*: (a) their purchase of sufficient identify-theft-prevention and credit monitoring services; (b) lower credit scores which have resulted or will result from, among other things, the large number of credit bureau inquiries associated with the actual and attempted thefts of their identities; (c) their purchase of credit-repair services; (d) their time spent monitoring their credit reports by nationwide consumer credit agencies; (e) their time spent

otherwise dealing with the numerous adverse effects of identity information theft; and/or (g) all other forms of economic harm and actual damages arising out of the theft of their confidential information.

98. As a direct and proximate result of the acts and omissions by Defendants described herein, Plaintiffs and the Class have suffered and/or will suffer significant non-economic harm including, *inter alia*, fear, anxiety and stress, where plaintiffs are entitled to actual and punitive damages.

COUNT IV
VIOLATION OF NEW HAMPSHIRE'S CONSUMER PROTECTION ACT, RSA 358-A

99. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

100. Defendants' conduct and violations of law constitute unlawful conduct within the meaning of RSA 358-A (hereinafter CPA).

101. Prior to the Date of Breach, Equifax promised to safeguard its consumers' PII, claiming that it had built its reputation on delivering reliable information to its customers and on protecting the privacy and confidentiality of personal information about consumers. In so doing, Equifax represented that its services have particular characteristics or benefits that they do not, and that those services are of a particular standard or quality that they are not.

102. Defendant violated the CPA, as alleged herein by failing to safeguard, and disclosing Plaintiffs' and Class Members' PII, and failing to provide adequate and timely notice of the disclosure. RSA 358-A:2, V, VII.

103. Defendant willfully and negligently violated the CPA, as alleged herein.

104. Defendant violated the CPA by engaging in unfair business practices by failing to implement appropriate procedures to guard against the release of class members' PII.

105. As a direct result of Defendant's violation of the CPA, Plaintiffs incurred distinct financial injuries.

106. Because Defendant's failure to adequately protect Plaintiffs' PII was willful and knowing, and because Defendant failed to disclose the breach for a lengthy period of time after it occurred, Plaintiffs are entitled to up to three times but not less than two times their damages.

107. Pursuant to RSA 358-A:10, Plaintiffs are further entitled to injunctive relief. Plaintiffs and the Class seek an order of this Court for equitable and/or injunctive relief in the form of an order:

a. Enjoining Defendants from continuing their unlawful practices described herein;

b. Directing Defendants to notify at its expense, with court supervision, all class members in full of the actual information stolen and/or potential theft of their identities as a result of the events underlying this class action;

c. Directing Defendants to implement security measures regarding private information that comply with the law;

d. Requiring Defendants to provide Plaintiffs' and Class Members' with:

(1) A lifetime of adequate identify theft prevention and credit monitoring services;

(2) Credit repair services;

(3) Sufficient identity theft insurance;

(4) Home security services;

(5) All other forms of restitution.

COUNT V
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. § 1681A(C).

108. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

109. As individuals, Plaintiffs and Class members are consumers entitled to the protections of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681a(c). Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

110. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

111. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

112. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

113. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Class members' PII.

114. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above. Equifax furnished Plaintiffs and the Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

115. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

116. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of

the measures organizations should take to prevent data breaches, and willingly failed to take them.

117. In addition, Equifax acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E.

118. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the class of their rights under the FCRA. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Class members' personal information for no permissible purposes under the FCRA.

119. Plaintiffs and the Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

120. Plaintiffs and the Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT VI

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

121. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

122. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches yet failed to take them.

123. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Class members' PII and consumer reports for no permissible purposes under the FCRA.

124. Plaintiffs and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

125. Plaintiffs and the Statewide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of the Statewide class)

126. Plaintiffs incorporate all prior paragraphs as if fully set forth herein.

127. Under the Declaratory Judgment Act, 28 U.S.C. § 2201 et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this complaint.

128. An actual controversy has arisen in the wake of Equifax's data breach regarding its common law and other duties to reasonably safeguard individuals PII. Plaintiffs allege that Equifax's data security measures were inadequate and remain inadequate.

129. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Equifax owed and continues to owe a legal duty to secure Class Members' personal and financial information and to notify Class Members of a data breach under the common law, Section 5 of the FTC Act and GLBA;

b. Equifax breached and continues to breach this legal duty by failing to employ reasonable security measures to secure Class Members' PII;

c. Equifax's breach of its legal duty proximately caused the data breach which it announced on September 7, 2017;

d. Equifax's continued failure to disclose exactly the scope of the data breach, and the individuals effected by the breach makes it impossible for class members to take appropriate measures to mitigate the risk of future identity theft;

e. Equifax's remedy to protect Class Members by offering consumers a free year of credit protection is insufficient.

130. The Court also should issue corresponding injunctive relief requiring Equifax to employ adequate security protocols to protect the PII of Class Members in its possession. Specifically, this injunction should, among other things direct Equifax to:

b. utilize industry standard secure default password and pin combinations in protecting individuals' PII;

c. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

d. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

e. regularly test its system for security vulnerabilities, consistent with industry standards;

f. immediately notify all Class Members of the data breach, and the scope of PII that was disclosed;

g. provide Class Members lifetime free credit protection.

131. If an injunction is not issued, Class Members will suffer irreparable injury and lack an adequate remedy in the event of another data breach, at Equifax. The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

132. The hardship to the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another data breach occurs at Equifax, the class will likely incur further risk of identity theft and fraudulent use of their PII. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security and notice measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

133. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Equifax, thus eliminating the injuries that would result to Class Members and others whose PII Equifax later obtains whose information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court grant Plaintiffs and Class Members the following relief against Defendant:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

B. Injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain PII to comply with the, the applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

C. An order requiring Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiffs and all Class Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiffs and all Class Members of a lifetime of credit monitoring and identity theft protection services provided by an entity other than Defendant;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order Requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other or further relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all issues in this action so triable of right.

Respectfully submitted,
JENNIFER GREENWALD, CYNTHIA ROBBINS, *ET AL*,
By their attorneys,

DOUGLAS, LEONARD & GARVEY, P.C.,

Date: September 21, 2017 By: /s/Charles G. Douglas, III

Charles G. Douglas, III (NH Bar #669)
14 South Street, Suite 5
Concord, NH 03301
(603) 224-1988
chuck@nhlawoffice.com